Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 654.026; 004.42

Романовский
Максим Сергеевич

Конфиденциальность передачи данных в средствах обмена сообщениями с использованием технологии blockchain

АВТОРЕФЕРАТ
диссертации на соискание ученой степени магистра технических наук
по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель
кандидат технических наук,
доцент Белоусова Е.С.

Минск, 2020

КРАТКОЕ ВВЕДЕНИЕ

Средства обмена сообщениями в режиме реального времени заняли серьёзное место в жизни человека. Данные программные продукты используются не только в качестве обмена сообщениями личного характера, а так же как способ делового общения. Не редко такие средства используются как корпоративная связь. Учитывая эти характеристики обеспечить безопасность и конфиденциальность передачи сообщений одна из главных задач разработчиков.

В настоящее время технология blockchain используется и поддерживается большим количеством крупных фирм. Преимущества этой технологии позволяют реализовать несложный функционал с надежной защитой. Использование blockchain технологии в разработке средства обмена сообщениями в режиме реального времени поможет сделать его конфиденциальным, целостным и доступным. Так же стоит учесть, что на сегодняшний день популярность приложений для обеспечения мгновенной передачи сообщений в глобальной сети является крайне высокой, поэтому актуальным является обеспечить защиту передачи таких сообщений.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 3.8 «Обеспечение цифрового доверия, защита информационных ресурсов и информационно-коммуникационной инфраструктуры» Стратегии развития информатизации в Республике Беларусь на 2016 – 2022 годы утвержденной на заседании Президиума Совета Министров от 03.11.2015 №26.

В диссертации поставлена и решена актуальная задача по совершенствованию безопасности передачи данных в средствах обмена сообщениями на основе использования технологии blockchain.

Практическая значимость работы состоит в том, что предложенное решение может повысить уровень конфиденциальности пользовательских данных при их передачи в средствах обмена сообщениями.

Цели и задачи исследования

Целью магистерской диссертации было обеспечение безопасности и конфиденциальности при передаче данных в средствах обмена сообщениями с использованием технологии blockchain.

В соответствии с поставленной целью, в работе сформулированы и решены следующие основные задачи:

– провести сравнительный анализ существующих средств обмена сообщениями, выявить их достоинства и недостатки;

– изучить уязвимости и слабые места приложений для обмена сообщениями между пользователями;

– разработать мобильное приложение на платформе Android с помощью современного языка программирования Kotlin на основе передовых подходов и технологий обеспечения безопасности и конфиденциальности передачи пользовательских данных;

– провести тестирование разработанного приложения на уязвимости.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на 56-ой конференции аспирантов, магистрантов и студентов Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (Минск, 2020).

Личный вклад соискателя

Содержание диссертации отображает личный вклад автора. Он заключается в научном обосновании использовании технологии blockchain для совершенствования безопасности передачи данных в средствах обмена сообщениями. Все основные результаты, выводы получены соискателем самостоятельно.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились с научным руководителем, кандидатом технических наук, доцентом Е.С. Белоусовой.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликована 1 работа, в том числе 1 тезисы доклада в сборнике материалов конференции.

Структура и объём диссертации

Диссертационная работа состоит из введения, общей характеристики работы, основной части из трех разделов, заключения, библиографического списка. Полный объём диссертационной работы составляет 57 страниц, включая 21 иллюстрации, список использованных источников из 15 наименований, список собственных источников из 1 наименования.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** определены основные направления исследований, обоснована актуальность темы диссертации, показана необходимость разработки средства обмена сообщениями в режиме реального времени и актуальность использования технологии blockchain для совершенствования безопасности передачи данных.

В **первой главе** приведены результаты сравнительного анализа существующих средств обмена сообщениями в режиме реального. Определено многообразие доступных на данный момент средств обмена сообщениями в режиме реального времени, выявлены их достоинства и недостатки. Решения, применяемые в ходе разработки такого вида приложений, часто требуют много временных и денежных затрат. Из проведенного сравнительного анализа сделан вывод, что все рассмотренные приложения не использует популярную и удобную в настоящее время технологию блокчейн. В тандеме со смарт-контрактами блокчейн позволяет быстро и эффективно разрабатывать приложения для обмена сообщениями в режиме реального времени, при этом такое приложение имеет высокую степень защиты, полную децентрализацию данных и их целостность. Исходя из этого, можно заключить, что актуальным является разработка мобильного приложения с использованием технологии blockchain.

Во **второй главе** дано описание выбранной платформы и языка программирования для разработки мобильного приложения. Проведенный анализ показал, что платформа Android становиться все более популярной как среди разработчиков, так и среди пользователей. Таким образом, можно сделать вывод, что разработка приложений для платформы Android может производится не только с использованием языка программирования Java или Kotlin, но и с использованием других языков программирования, что делает процесс разработки еще более доступным для большего количества разработчиков. Произведено изучение средств разработки, которые ориентированы на начинающих разработчиков, или которые могут использоваться в учебных целях. Большинство рассмотренных средств программирования являются либо свободно распространяемыми, либо условно-бесплатными, что тоже повышает популярность платформы Android.

В **третьей главе** описывается процесс разработки средства обмена сообщениями в режиме реального времени. Акцент делается на модульную разработку с использованием современных подходов. Так же описан процесс тестирования и представлены результаты тестирования, которые подтверждают функциональность разработанного мобильного приложения и высокий уровень безопасности передаваемых пользовательских данных.

ЗАКЛЮЧЕНИЕ

На основе проведённого анализа существующих средств обмена сообщениями в реальном времени был сделан вывод, что каждое анализируемое средство имеет сложную архитектуру и широкий функционал, разработка которых потребовала большого количества временных и денежных затрат. Изучение недостатков современных средств обмена сообщениями позволил избежать их при реализации мобильного приложения с использованием технологии. Выбор и внедрение технологии blockchain в разрабатываемое мобильное приложения обусловлен преимуществами этой технологии, а именно децентрализованность и высокий уровень защищённости, что позволяет разработать аналог существующих средств обмена сообщениями в режиме реального времени с использованием меньшего количества ресурсов.

В качестве платформы для реализации мобильного приложения была выбрана ОС Android. Открытый код данной платформы, большое количество разработчиков, а так же сильная поддержка со стороны разработчиков самой платформы позволяет пользоваться большим количеством готовых решений. В качестве языка программирования выбор стоял между Kotlin и Java. Так как Kotlin компилируется в Java, было уместнее выбрать именно его. По сравнению с Java добавлены многие полезные и удобные синтаксические и функциональные решения. Так же разработка мобильного приложения на данном языке программирования в целом удобнее и быстрее.

Разработка средства для обмена сообщениями в режиме реального времени происходила по модулям. Разделения на модули было выбрано по функциональным сходствам. Такой подход позволил фокусироваться на конкретных задачах и ускорил процесс. Так же в дальнейшем это положительно сказалось на тестировании приложения. Для отображения информации на экране был выбран эргономичный дизайн, соответствующий современным тенденциям. В процессе тестирования не было выявлено логических и функциональных проблем в работе приложения.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Романовский, М.С. Особенности разработки мобильного приложения для защищённого обмена сообщениями в режиме реального времени с использование технологии blockchain / М.С. Романовский, Е.С. Белоусова // 56-я конференция аспирантов, магистрантов и студентов Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 18-20 мая 2020 г., БГУИР, Минск, Беларусь: тезисы докладов. – М. – 2020. – С. 41.